GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

IGF GENEVA 2017

www.cyberstability.org | info@cyberstability.org | cyber@hcss.nl | @theGCSC

THE PUBLIC CORE PRINCIPLE

SUBMISSION TO THE 2017 IGF-BPF CYBERSECURITY BY THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE

The Internet was described in the 2003[1] as being a "global facility". What this means has never been adequately determined, although a number of prominent statements have been made over the past years that have described the Internet as representing in whole or in part a "global commons". The Global Commission on the Stability of Cyberspace (GCSC) has investigated the question, and is favoring the concept of a "Public Core" of the Internet.[2] We are open to expanding this concept to that of an operational principle, such as those that have been put forward as Core Values by the IGF Dynamic Coalition on Core Internet Values[3] or described as Internet Invariants by ISOC.[4]

The GCSC submits that the Internet is a common good for humanity.[5] Parts of the Internet further conform to the notion of a "global public good", providing essential functionality to the Internet as a whole and which underpins its normal operation. If one or more of these core functionalities are undermined or disrupted, then the security and stability of the Internet can be significantly impacted, decreasing trust and confidence in the domain amongst all stakeholders. These core functionalities are encapsulated in the concept of the "Public Core".

Following the original WRR study on the Public Core, the author of the concept Dennis Broeders sketched out some further ideas at a public hearing of the GCSC Full Commission Meeting in Tallinn in May 2017. At his hearing, Broeders defined the core as encompassing two elements: (i) a clearly distinguishable "Inner Core" which consists of the core functionality underpinning the Internet (in particular the forwarding and naming functions and infrastructure of the Internet and those actors responsible for their day to day management[6]), and (ii) a less clearly distinguishable "Outer Core" of

---

[1] WSIS Geneva Declaration #48 (2003)

[2] The Public Core concept was elucidated in a 2015 study by the Netherlands Scientific Council for Public Policy (WRR) : https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet . The author has since updated some of the work in 2017 publication: http://cf.orfonline.org/wp-content/uploads/2017/07/ORF_IssueBrief_190_PublicCore.pdf

[3] See www.coreinternetvalues.org

[4] See https://www.internetsociety.org/internet-invariants-what-really-matters/

[5] For a wider discourse analysis on the terms "good for humanity", "common heritage of mankind", "global public good and public resource" as we all as "global commons", please see Appendix B.

[6] This refers also to the "naming and forwarding functions" which encapsulates naming and addressing as well as routing and switching technology. It encapsulates the security and stability of key protocols (in particular DNS, BGP, IPv6 and others), the operation of the Domain Name System (including those of all Top Level Domains), and the operation of the Root Zone. It may potentially be expanded to include the infrastructure it depends upon – such as the Root Zone operators themselves, their equipment, and the physical connections between them.

potentially critical functionality, whose impact on the overall stability and security of the Internet as a whole may be uncertain, or which may fluctuate depending on circumstances.

For the basic definition, the GCSC has largely concluded it deliberations around a proposed norm[7] of behavior to be considered by all stakeholders in its "Call to Protect the Public Core of the Internet"[8]:

> *"Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace".*[9]

The GCSC welcomes feedback on this norm, both in terms of wording as well as possible levers for implementation. Many different variants of the above were considered. The present wording of the protective norm above is considered wide enough that it would encapsulate both clearly identifiable core functions (such as the naming and forwarding functions) but also allow other definitions to take root. Indeed, one interpretation of the norm is that it gives rise to a general precautionary principle applicable to all actors to be exercised by all stakeholders whose standards, products, services, legislations or policy initiatives could reasonably become critical to the overall security and stability of the overall functionality of the Internet. This principle would encourage a higher standard of duty of care – for instance in considering security issues at the design stage – for all actors whose new standards, products, services, legislations or policies could reasonably be assessed as *potentially* becoming critical for the functioning of the Internet as a whole. In the best case, this could become known as the "Public Core Principle", the reinforcement of the "Do No Harm Principle" to all Internet stakeholders.

The GCSC welcomes input on the entire Public Core concept, including especially (i) the norm, its implications, and options for implementation and reinforcement and (ii) the potential for developing a general precautionary Public Core Principle that would apply to all Internet stakeholders.

Two further documents have been included; Appendix A, which lists possible application of the principle, and Appendix B, which provides a backgrounder on the various usages of "global public good" and other related terminology.

---

[7] Norms are voluntary, non-binding commitments. Over time they can crystallize into international law. Norms prescribe a positive or a negative obligation. The overall stability of the cyberspace is also served through capacity and confidence building efforts.

[8] GCSC Commissioners issued a "Call to Protect the Public Core of the Internet" at the Commission Meeting in New Delhi in November 2017, urging state and non-state actors to avoid activity that would intentionally and substantially damage the general availability or integrity of the "public core" of the Internet.

[9] Elements of the public core include, inter alia, Internet routing, the domain name system, certificates and trust, and communications cables.

THE PUBLIC CORE PRINCIPLE APPENDIX A: STAKEHOLDER RELEVANCE

The Public Core Principle could be applied equally to all operational stakeholders and to both the Inner Core and Outer Core described above. The following is to be considered as food for thought in assessing what the Pubic Core Principle could mean in practice.

- *Governments* are increasingly asserting their offensive capabilities in cyberspace. In theory, some of these capabilities can have a direct impact on the stability of the Internet. This can occur directly, for instance where governments may seek to misuse key protocols for so-called Man-on-the-Side attacks. But it also can occur indirectly, for example by knowingly allowing vulnerabilities in the Public Core (e.g. key Internet protocols such DNS and BGP) to remain unpatched, therefore potentially encouraging malfeasance by other actors. Special attention should be paid in the development of offensive cyber capabilities ("cyber weapons"), including in the deployment of autonomous malware that limits the potential impact of their use on the core functionality of the Internet. Further, the precautionary Principle indicates that governments should take special care to avoid inadvertent escalation in tensions in cyberspace due to misinterpretation of motives and actions by other States. Governments should also not support legal or policy initiatives that potentially could unbalance the current technical Internet governance standard-setting process, or introduce national legislation that effectively disrupts the functioning of the organizations responsible for crucial naming and forwarding functions.

- *The Private Sector* has a special stake in the decrease of offensive operations in cyberspace, and has become increasingly outspoken in the need for this to occur.[10] However, the private sector also plays an important role in the Inner Core of the Internet, especially in maintaining the root zone as well as the routing and switching (together *forwarding*) of Internet traffic. Companies that play a part in the Inner Core should consider their naming and forwarding responsibilities not as being principally subject to commercial logic, but ought to take into account the general availability, integrity, and functionality of global ICT systems. Similarly, the private sector accounts for the bulk of actors whose products and services position themselves within the "Outer Core". Companies across the spectrum of commercial activity – from routing, networking, hardware manufacturing, service provisioning, all variants of software vending and similar – need to be aware of what potential impact the misuse of their product or services may have for the core functionalities of the Internet. If there is a reasonable expectation that their services or products could potentially be misused to undermine the basic stability and security of the Internet, these companies should apply a higher standard of care in both design and delivery of these services or products. Similarly, if a service can be introduced that, at marginal cost to the implementer, provides a meaningful benefit to the overall security and stability of the Internet, then, in accordance with the Principle, the service should be implemented even if the implementer has no direct gain from it.[11] Finally, the private sector has strong overlap with the civil society (including the technical community and academia) and it should seek to support its employees when they engage in these activities on their own volition, and to support and not undermine their independence.

---

[10] Recent submissions by Mozilla, Microsoft and others show that the private sector is taking an increasingly vocal position on the need to commonly protect the Internet from malicious actors.

[11] A very timely example is the repeated call for ISPs to implement Source Address Validation (SAV) on their systems. This could potentially reduce the effectiveness of most DDoS attacks. However, in a classic case of the principle agent problem, international implementation has been slow due to fact that implementing SAV does not protect the ISP in question itself, only its neighbors (and competitors). One exception for this has been China, where the government simply mandated the implementation of SAV on all ISPs.

- *The civil society, the technical community, and academia* remain the genesis for most of the protocols and standards that lie at the heart of the Inner Core, and provides the trusted community representatives that authenticate it. The civil society has shown that it executes these responsibilities (such as the root zone authentication process[12]) with the utmost due diligence, and has developed protocols and systems to keep its availability, functionality, and integrity intact. Nonetheless the civil society is under increasing pressure both externally and internally. When working with the Inner Core, standard setting groups need to be aware of the potential security implications (including threats to human rights) of their work. To date, the IETF and other standard setting groups have been able to deftly avoid or reverse potentially risky RFCs, but this requires consistent vigilance. In response to the need to update and expand the existing Internet governance mechanisms to make them more inclusive, it is important to be able to maintain the flexibility of the current process that has so far been resilient to both co-option as well as serious missteps in the design of standards.

[12] Trust Community Representatives play a key role in the cryptographic signing of the root zone.

THE PUBLIC CORE PRINCIPLE APPENDIX B: GLOBAL PUBLIC GOODS

The genesis of the Public Core Principle lies with repeated assessments of the Internet, or parts of the Internet, as representing a "global commons" or a "global public resource". A slightly less encompassing definition is that of a "global public *good*" – which according to some interpretations does not represent a global commons.

The definition of the Internet or parts of it as a "global public good" was explicitly mentioned as early as 1999 in a report for the UNDP, where it was suggested that the architecture of cyberspace appears to fit the standard economic definition of a "public good".[13] Since then, the WSIS Geneva Declaration #48 (2003) stated that the Internet has evolved into a global facility available to the public and its governance should constitute a core issue of the Information Society agenda. In a statement, the ITU Secretary-General (March 2014) reiterated that "the Internet is a global public good and therefore all nations and peoples should have an equal say in its running and development." In 2014, Neelie Kroes, then European Commissioner for the Digital Agenda, referred to the Internet as a "global, common, public resource and its governance must be truly global, transparent and accountable." In April 2014, the NETmundial Multistakeholder Statement "recognized that the Internet is a global resource which should be managed in the public interest". Later on, the 2016 OECD Cancún Declaration, further recognizes "the important contribution of the Internet Governance Principles of the NETmundial Multistakeholder Statement", which included the description of the Internet as a global public resource. In May 2015, during a keynote speech at Cycon15 in Estonia, NSA and CYBERCOM director Adm. Michael Rogers referred to the Internet as a "a global commons that enables open, reliable, safe and resilient communications", including the mentioning of an Internet interpretation model based on the Law of the Sea. In September 2015, the German Foreign Minister Steinmeier stated that the Internet is a "global public good" that needs to be protected. Dennis Broeders argues that the Internet's key protocols can be considered a global public good in his book *The Public Core of the Internet*. During the UNGA High-level meeting of the WSIS+10 review at the end of 2015, Malta referred to the internet as a global public resource, and argues in favor of the legal concept of the Common Heritage of Mankind to be applied to critical infrastructures of the Internet by analogy with Article 136 of the United Nations Convention on the Law of the Sea. Ecuador, speaking on behalf of the Community of Latin American and Caribbean States, considered that the Internet should be an open global public good, and Finland stated that the Internet should be protected and nurtured as a global public good. In early 2016, World Development Report refers to the Internet as both a subject of co-operation and a new tool to facilitate co-operation in other realms. In its final report *One Internet*, the Global Commission on Internet Governance argues that parts of the Internet constitute a shared global public good in claiming that the Internet's future ultimately depends on a 'new social compact', which would ensure "that the Internet continues on track to become more accessible, inclusive, secure and

[13] Previously there were many similar statements that did not fit the definition verbatim, but came very close in practice. A general understanding of the Internet as a "global public good" evolved in the ISOC discussions in the 1990s and was seen as a starting point in the negotiations towards the IAHC gTLD MoU where ISOC, IANA and IAB/IETF agreed with ITU, WIPO and INTA in 1997. Section 2 of the MoU from 1997 included a paragraph that stated, inter alia "the Internet TLD space is a public policy issue and should be carried out in the interests and service of the public". This MoU was never ratified, and instead ICANN included this concept into its "Articles of Incorporation" in 1998. Section 3 of the original Articles from 1998 stated: "In furtherance of the foregoing purposes, and in recognition of the fact that the Internet is an international network of networks, owned by no single nation, individual or organization, the Corporation shall ... pursue the charitable and public purposes of lessening the burdens of government and promoting the global public interest in the operational stability of the Internet." Even in 1998 this was not a new idea. This idea was discussed in the context of the G7 meeting in Brussels in 1995 and was part of the US proposal for a "Global Information Infrastructure Initiative" (GII), which was presented by US Vice President Al Gore during the ITU-WTDC in Buenos Aires in 1994.

trustworthy." Mozilla emphasized that the "internet is a global public resource" in February 2016. At the 14th Meeting of Foreign Ministers of Russia, India and China, the three countries issued Joint Communiqué in which they considered the Internet a global resource, and later that year, leaders of the BRICS reaffirm that the Internet is a global resource in the Goa Declaration.

With one notable exception (the speech by the then newly appointed director of NSA/USCYBERCOM in 2015 recounted above) the governmental references to the Internet as a whole as being part of a global public resource (i.e. "global commons") are concentrated among BRICS nations. Most other governments and international organizations speak instead of a "global public good". The EU is among a few actors that instead have taken to referring to the Internet as constituting "a common good for humanity".[14] All three definitions have specific expectations tied to them. The definition of the Internet as a "global public good" indicates that it is not possible to exclude individual actors from the use of the Internet, while defining it as "global public resource" (or common pool resource) implies that it is possible. In both cases government intervention is sanctioned, but for different reasons: in case of a "global public good", government intervention is primarily important to address the impact of a free-rider problem[15], while in case of the "global public resource", the implication is that government intervention is important to prevent the exclusion of one nation from the Internet by another. The third usage, namely that of referring to the Internet as representing "common good for humanity", is closest to a concept in International Law, the Common Heritage of Mankind (CHM) principle. The CHM principle holds that defined territorial areas and elements of humanity's common heritage (cultural and natural) should be held in trust for future generations and be protected from exploitation by individual nation states or corporations.[16]

The Public Core Principle sidesteps any kind of discussion as to how much of the Internet infrastructure is to be considered a "global commons" and therefore in need of special (inter)governmental protection. It does however highlight that the Internet depends on core functionalities – functionalities that should be immune to any kind of political or commercial aspirations and which should empower a "dumb" network that is agnostic to all. This Public Core is not only under threat by governments, although governments are increasingly showing their presence in cyberspace. It is also equally prone to disruption due to commercial aspirations or even the failure of the civil society and technical community structures that have built and maintained it. Protecting the Public Core is therefore a task for all actors, and all actors need to assume responsibility for it – not only in its clearly defined Inner Core, but also as an overriding precautionary Principle as well.

---

[14] "The internet is a common good for humanity and ensuring its good governance will help bring its benefits to all people in the world", said European Commission Vice President Andrus Ansip and Members of the European Parliament in a joint declaration. The statement was signed by the EU delegation in Brazil during the 10th Internet Governance Forum.

[15] The free rider problem in cyberspace can be phrased in economic but also security terms. In security terms, the primary free rider problem is that governments face little apparent cost (politically or financially) to increasing leveraging cyberspace to address national security issues – both domestic and foreign.

[16] The CHM principle was applied first to the Law of the Seas, where it was important in helping define a regulative framework for exploiting the deep seabed. The concern at the time was that technically advanced parties would have the ability to exploit these resources first, and therefore deny less advanced parties the ability to do so in the future. The CHM principle was an attempt to indicate that any exploitation of the advanced parties should also benefit those parties who are were not able to directly exploit them at the time. Similarly, the CHM principle was later applied to prevent the one-sided exploitation of the Antarctic as well as Outer Space. Most recently, it has been adopted in world heritage conventions as well as conventions protecting the human genome from one-sided exploitation. There is some debate on how effective the CHM principle has been to date. Nonetheless there have been reoccurring attempts to reintroduce it in the context of cyberspace. See for instance the Maltese submission to the UN:
https://www.gov.mt/en/Government/Press%20Releases/Documents/pr152897a.pdf